Доклады Академии Наук СССР
1950. Том LXXIV, № 3

МАТЕМАТИКА

А. И. СКОПИН

ФАКТОР-ГРУППЫ ОДНОГО ВЕРХНЕГО ЦЕНТРАЛЬНОГО РЯДА СВОБОДНОЙ ГРУППЫ

(Представлено академиком В. И. Смирновым 29 VII 1950)

Работа посвящена следующему вопросу: для свободной группы $\mathfrak{G}$ с k образующими строится последовательность нормальных делителей $\mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \ldots$ индуктивно следующим образом:
1) $\mathfrak{G}_{i-1}/\mathfrak{G}_i$ есть элементарная абелева p-группа, $p \neq 2$;
2) $\mathfrak{G}_{i-1}/\mathfrak{G}_i$ лежит в центре $\mathfrak{G}/\mathfrak{G}_i$;
3) $\mathfrak{G}_i$ есть минимальная группа, обладающая свойствами 1) и 2)
Исследуются фактор-группы $\mathfrak{G}_{i-1}/\mathfrak{G}_i$.

В работе используется представление свободной группы в кольце формальных степенных рядов от k ассоциативных переменных как группы, порожденной элементами $1+x_i$, $i=1, 2, \ldots, k$, относительно умножения в кольце, причем $(1+x_i)^{-1} = 1 - x_i + x_i^2 - \ldots$.

Будем употреблять следующие обозначения: P_m — однородный полином с целыми коэффициентами степени m в образующих x_i L_m — однородный полином Ли с целыми коэффициентами степени m в образующих x_i относительно умножения Ли:

$$x \circ y = xy - yx.$$

Если $\mathfrak{A}$ — группа, то $\mathfrak{A}^m$ — ее нормальный делитель, порожденный m-ми степенями всех ее элементов; $a^{(m)}$ — элемент $\mathfrak{A}^m$.

Если $\mathfrak{M}$ и $\mathfrak{N}$ — подмножества $\mathfrak{A}$, то $[\mathfrak{M}, \mathfrak{N}]$ — нормальный делитель $\mathfrak{A}$, порожденный образованиями вида $[m, n] = mnm^{-1}n^{-1}$ $(m \in \mathfrak{M},\ n \in \mathfrak{N})$.
Используются следующие результаты статьи ([1]):

M_1. Группа $\mathfrak{G}$ свободна в образующих $1+x_i$, $i=1, 2, \ldots, k$.

M_2. Каждый элемент $\mathfrak{G}$ имеет вид $1+L_n+P_{n+1}+\ldots$, где под точками, как и везде в дальнейшем, подразумеваются слагаемые более высоких степеней, чем написанные. L_n может быть любым.

M_3. Каждый элемент $\mathfrak{G}$ вида $1+L_n+\ldots$ принадлежит к $\mathfrak{G}^{(n-1)}$, $(n-1)$-му члену верхнего центрального ряда $\mathfrak{G}^{(0)} \supset \mathfrak{G}^{(1)} \supset \ldots$, образованного по закону $\mathfrak{G}^{(0)} = \mathfrak{G}$; $\mathfrak{G}^{(n)} = \left[\mathfrak{G}^{(n-1)}, \mathfrak{G}\right]$, и обратно, любой элемент $\mathfrak{G}^{(n-1)}$ имеет вид $1+L_n+\ldots$

M_4. Если g, $g' \in \mathfrak{G}$ и $g = 1+L_n+\ldots$, $g' = 1+L'_n+\ldots$, то $gg' = 1+L_n+L'_n+\ldots$

Теорема 1.

$$\mathfrak{G}_n = \mathfrak{G}_{n-1}^p [\mathfrak{G}_{n-1}, \mathfrak{G}].$$

Доказательство. Очевидно, что если $\mathfrak{G}_{n-1}$ уже построено, то $\mathfrak{G}_n$ есть ядро гомоморфизма:

$$g_{n-1} \to g_{n-1} [\mathfrak{G}_{n-1}, \mathfrak{G}] \to g_{n-1} [\mathfrak{G}_{n-1}, \mathfrak{G}] (\mathfrak{G}_{n-1} / [\mathfrak{G}_{n-1}, \mathfrak{G}])^p, \quad g_{n-1} \in \mathfrak{G}_{n-1},$$

переводящего $\mathfrak{G}_{n-1}$ в

$$\mathfrak{G}_{n-1} / [\mathfrak{G}_{n-1}, \mathfrak{G}] \Big/ (\mathfrak{G}_{n-1} / [\mathfrak{G}_{n-1}, \mathfrak{G}])^p.$$

Но $(\mathfrak{G}_{n-1} / [\mathfrak{G}_{n-1}, \mathfrak{G}])^p$ состоит из смежных классов $g_{n-1}^{(p)} [\mathfrak{G}_{n-1}, \mathfrak{G}]$, т. е. элементы из $\mathfrak{G}_{n-1}^p [\mathfrak{G}_{n-1}, \mathfrak{G}]$ переходят в единицу. Обратно, если g_{n-1} переходит в единицу, то $g_{n-1} [\mathfrak{G}_{n-1}, \mathfrak{G}] \in (\mathfrak{G}_{n-1} / [\mathfrak{G}_{n-1}, \mathfrak{G}])^p$, т. е. $g_{n-1} = g'g''$, где $g' \in \mathfrak{G}_{n-1}^p$ и $g'' \in [\mathfrak{G}_{n-1}, \mathfrak{G}]$. Теорема доказана.

Теорема 2. *Каждый элемент $\mathfrak{G}_n$ имеет вид:*

$$g_n = 1 + \sum_{i=1}^{n+1} p^{n-i+1} P_i + \ldots, \qquad (*)$$

где $P_i \equiv L_i \pmod p$, $i = 1, 2, \ldots, n+1$.

Доказываем теорему по индукции. Для $\mathfrak{G}_0 = \mathfrak{G}$ теорема верна. Пусть она верна для $\mathfrak{G}_{n-1}$. Возьмем произвольное $g_n \in \mathfrak{G}_n$. По теореме 1, $g_n = g'g''$, где $g' \in \mathfrak{G}_{n-1}^p$ и $g'' \in [\mathfrak{G}_{n-1}, \mathfrak{G}]$.

1. Докажем, что p-я степень элемента $\mathfrak{G}_{n-1}$ удовлетворяет $(*)$.

Обозначим $g_{n-1} = 1 + \sum\limits_{i=1}^{n} p^{n-i} P_i + \ldots = 1 + A$. Здесь $P_i \equiv L_i \pmod p$, $i = 1, 2, \ldots, n$. Тогда $g_{n-1}^p = 1 + pA + pA^2 Q + A^p$ (из формулы бинома Ньютона), где Q — полином с целыми коэффициентами.

Ясно, что $1 + pA = 1 + \sum\limits_{i=1}^{n} p^{n-i+1} P_i + pP_{n-1} + \ldots$ удовлетворяет $(*)$.

Полином с целыми коэффициентами будем называть несущественным для $(*)$, если его коэффициенты при слагаемых степени i делятся на p^{n-i+2}.

От прибавления таких полиномов выражения P_i, входящие в $(*)$, не меняются по модулю p. Полином, очевидно, останется несущественным для $(*)$, если его домножить на полином с целыми коэффициентами. Покажем, что $pA^2Q + A^p$ несущественный для $(*)$ полином.

$$A^2 = \left(\sum_{i=1}^{n} p^{n-i} P_i + \ldots \right)^2 = \sum_{i,j=1}^{n} p^{2n-i-j} P_i P_j + \ldots$$

Группируя слагаемые по степеням, будем иметь:

$$A^2 = \sum_{i=1}^{n+1} p^{2n-i} P_i^{(1)} + \ldots,$$

ибо слагаемые до $(n+1)$-й степени получаются только из P_i, $i \leqslant n$.

$$A^2 = p^{n-1} \sum_{i=1}^{n+1} p^{n-i+1} P_i^{(1)} + \ldots$$

Следовательно, $pA^2 = p^{n-1} \sum\limits_{i=1}^{n+1} p^{n-i+2} P_i^{(1)} + \ldots$, что несущественно для $(*)$ в силу $n \geqslant 1$.

Аналогично преобразуем $A^p = A^3 Q^{(1)}$ (так как $p \geqslant 3$):

$$A^3 = \left(\sum_{i=1}^{n} p^{n-i} P_i + \ldots \right)^3 = \sum_{i,j,k=1}^{n} p^{3n-i-j-k} P_i P_j P_k + \ldots =$$

$$= \sum_{i=1}^{n+1} p^{3n-} P_i^{(2)} + \ldots = p^{2n-2} \sum_{l=1}^{n+1} p^{n-i+2} P_i^{(2)} + \ldots,$$

т. е. несущественно для (*).

2. Покажем, что коммутатор $[g_{n-1}, g]$ удовлетворяет (*). Для доказательства воспользуемся формулой:

$$(1+x)(1+y)(1+x)^{-1}(1+y)^{-1} = 1 + (x \circ y)(1+x)^{-1}(1+y)^{-1},$$

которая очевидна из

$$(1+x)(1+y) - (1+y)(1+x) = xy - yx = x \circ y.$$

Имеем

$$g_{n-1} = 1 + \sum_{i=1}^{n} p^{n-i} P_i + \ldots,$$

$$g = 1 + L_s + \ldots,$$

откуда, в силу вышесказанного,

$$[g_{n-1}, g] =$$

$$= 1 + \left[\left(\sum_{i=1}^{n} p^{n-i} P_i + \ldots \right) \circ (L_s + \ldots) \right] (1 + p^{n-1} P_1 + \ldots)^{-1} (1 + L_s + \ldots)^{-1} =$$

$$= 1 + \sum_{i=1}^{n} p^{n-i} P_i \circ L_s + \ldots .$$

Только записанные слагаемые и только при $s = 1$ будут существенными для (*), так как остальные, имея степень не ниже $i + 2$, делятся на p^{n-i}. Таким образом,

$$[g_{n-1}, g] = 1 + \sum_{i=2}^{n+1} p^{n-i+1} P_i^{(3)} + \ldots,$$

где $P_i^{(3)} \equiv P_i \circ L_1 \pmod p$, если $s = 1$, и $P_i^{(3)} \equiv 0 \pmod p$, если $s \geqslant 2$, т. е. $[g_{n-1}, g]$ имеет требуемый вид. Для полного доказательства теоремы 2 теперь достаточна теорема 3.

Теорема 3. *При перемножении элементов $\mathfrak{G}$ вида (*) полиномы P_i, $i = 1, 2, \ldots, n+1$, складываются по модулю p.*

Проверяем:

$$\left(1 + \sum_{i=1}^{n+1} p^{n-i+1} P_i + \ldots \right) \left(1 + \sum_{i=1}^{n+1} p^{n-i+1} P_i^{(1)} + \ldots \right) = (1 + A)(1 + A^{(1)}) =$$

$$= 1 + A + A^{(1)} + AA^{(1)} = 1 + \sum_{i=1}^{n+1} p^{n-i+1} (P_i + P_i^{(1)}) + \ldots + AA^{(1)}.$$

$$AA^{(1)} = \left(\sum_{i=1}^{n+1} p^{n-i+1} P_i + \ldots \right) \left(\sum_{j=1}^{n+1} p^{n-j+1} P_j^{(1)} + \ldots \right) =$$

$$= \sum_{i,j=1}^{n+1} p^{2n+1-i-j+1} P_i P_j + \ldots = p^{n+1} \sum_{i=1}^{n+1} p^{n-i+1} P_i^{(2)} + \ldots,$$

что несущественно для $(*)$ из-за $n \geqslant 0$, и теоремы 2 и 3 доказаны.

Лемма. *В $\mathfrak{G}_n$ существует элемент вида*

$$1 + p^{n-i+1}L_i + \ldots \quad (1 \leqslant i \leqslant n+1),$$

где L_i — любой.

Доказательство. По M_3, существует $1 + L_i + \ldots \in \mathfrak{G}^{(i-1)}$. Очевидно, $\mathfrak{G}^{(m)} \subset \mathfrak{G}_m$, ибо $\mathfrak{G}^{(0)} = \mathfrak{G}_0 = \mathfrak{G}$, и, если $\mathfrak{G}^{(n-1)} \subset \mathfrak{G}_{n-1}$, то $\mathfrak{G}^{(n)} = [\mathfrak{G}^{(n-1)}, \mathfrak{G}] \subset [\mathfrak{G}_{n-1}, \mathfrak{G}] \subset \mathfrak{G}_{n-1}^p [\mathfrak{G}_{n-1}, \mathfrak{G}] = \mathfrak{G}_n$.

По M_4:

$$(1 + L_i + \ldots)^{p^{n-i+1}} = 1 + p^{n-i+1}L_i + \ldots \in (\mathfrak{G}^{(i-1)})^{p^{n-i+1}} \subset \mathfrak{G}_{i-1}^{p^{n-i+1}} \subset \mathfrak{G}_n$$

(последнее включение из-за $\mathfrak{G}_{k-1}^p \subset \mathfrak{G}_{k-1}^p [\mathfrak{G}_{k-1}, \mathfrak{G}] = \mathfrak{G}_k$ $(k = 1, 2, \ldots)$). Лемма доказана.

Теорема 4. *Каждый элемент $\mathfrak{G}$ вида $(*)$ принадлежит к $\mathfrak{G}_n$.*

Доказательство. Пусть $g = 1 + p^n P_1 + \ldots + pP_n + P_{n+1} + \ldots \in \mathfrak{G}$, $P_i \equiv L_i \pmod p$, $i = 1, 2, \ldots, n+1$. Так как $P_1 = L_1$, то, по лемме, существует $g_1 = 1 + p^n P_1 + \ldots \in \mathfrak{G}_n$; по теореме 2, g_1 имеет вид $(*)$, следовательно, по теореме 3, $g g_1^{-1} = 1 + p^{n-1} P_2^{(1)} + \ldots$ имеет вид $(*)$.

По M_2, $P_2^{(1)} = L_2^{(1)}$. Снова применяем лемму: $g g_1^{-1} g_1^{-1} = 1 + p^{n-2} P_3^{(2)} + \ldots$ имеет вид $(*)$.

Окончательно получим: $g g_1^{-1} \ldots g_n^{-1} = 1 + P_{n+1}^{(n)} + \ldots$, где $g_1, g_2, \ldots, g_n \in \mathfrak{G}_n$, но, по M_3, $1 + P_{n+1}^{(n)} + \ldots \in \mathfrak{G}^{(n)} \subset \mathfrak{G}_n$, значит, и $g = (1 + P_{n+1}^{(n)} + \ldots) g_n g_{n-1} \ldots g_1 \in \mathfrak{G}_n$, что и требовалось.

Теорема 5 (основная),

$$\mathfrak{G}_n / \mathfrak{G}_{n+1} \cong L_1 + \ldots + L_{n+1} / p (L_1 + \ldots + L_{n+1}),$$

где L_m — модуль однородных полиномов Ли степени m с целыми коэффициентами.

Доказательство. Сделаем следующее отображение $\mathfrak{G}_n$ на $L_1 + \ldots + L_{n+1} / p (L_1 + \ldots + L_{n+1})$:

$$g_n = 1 + p^n P_1 + \ldots + pP_n + P_{n+1} + \ldots \to L_1 + \ldots L_n + L_{n+1},$$

где $P_i \equiv L_i \pmod p$, $i = 1, 2, \ldots, n+1$.

По построению и теореме 2 это отображение однозначно. По теореме 3 оно — гомоморфизм. По теоремам 2 и 4 ядром этого гомоморфизма является $\mathfrak{G}_{n+1}$.

Ленинградский государственный университет
им. А. А. Жданова

Поступило
18 VII 1950

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] W. Magnus, Math. Ann.. 111, 259 (1935).